Révision de la règlementation européenne sur la protection des données personnelles

Boris Barraud

Aix*Marseille université

L.I.D.2 M.S.
Laboratoire Interdisciplinaire de Droit des Médias & des Mutations Sociales

Boris Barraud, « Révision de la règlementation européenne sur la protection des données personnelles », *Revue Européenne des Médias et du Numérique* 2016, n° 38, p. 14 s.

manuscrit de l'auteur

HAL
SCIENCES DE L'HOMME ET DE LA SOCIÉTÉ

Le 14 avril 2016, le Parlement européen a définitivement adopté le projet de « paquet législatif » relatif à la protection des données personnelles. Celui-ci comporte un règlement et une directive qui sont appelés à faire sensiblement évoluer le droit des données personnelles des États membres de l'Union européenne au cours des prochaines années.

Le régime juridique européen des données personnelles, issu de la directive 95/46/CE du 24 octobre 1995, est apparu de plus en plus dépassé au cours des années 2000, à mesure que les nouvelles technologies de l'information et de la communication et leurs usages se sont développés. Avec l'avènement de l'internet et du Big Data, la protection des données personnelles est devenue un enjeu de société majeur, posant des questions telles que celle du droit à l'oubli ou celle de la surveillance de masse. Chaque citoyen européen est aujourd'hui concerné, ce qui en fait l'un des dossiers les plus importants parmi ceux que l'Union européenne a à traiter.

Aussi cette dernière a-t-elle entendu réformer la directive de 1995. Pour cela, elle a souhaité recourir à l'instrument du règlement, lequel, à l'inverse de la directive, est directement applicable parmi les États membres sans besoin de transposition préalable — chacun pourra donc se prévaloir de ce texte à portée générale et contraignant sitôt qu'il sera entré en application —. Le règlement permet mieux que la directive de lutter contre la fragmentation juridique, très préjudiciable dès lors qu'il s'agit de saisir des objets transnationaux tels que les communications par internet.

Initiée par la Commission européenne le 25 janvier 2012, la réforme du droit européen de la protection des données personnelles a ensuite donné lieu à de longues et lourdes négociations entre cette Commission, le Conseil de l'Union européenne et le Parlement européen, ainsi qu'à l'intérieur de chacun de ces organes. En témoigne le nombre record d'amendements à la proposition de règlement déposés : 3999. Ces négociations ont pris fin le 15 décembre 2015 et c'est finalement le 14 avril 2016 que le Parlement a définitivement adopté le projet, à la suite du Conseil qui s'était prononcé favorablement le 8 avril précédent.

Outre un règlement général, le nouveau « paquet législatif » relatif à la protection des données personnelles comporte une directive visant à établir un cadre juridique européen pour les transferts de données à des fins policières et judiciaires. Le règlement sur la protection des données est entré en vigueur 20 jours après sa publication au Journal officiel de l'Union européenne ; ses dispositions seront directement applicables dans tous les États membres deux ans après cette date, soit en avril 2018. Quant à la directive, les États disposent de deux ans pour transposer ses dispositions dans leurs droits nationaux.

Le premier objectif : renforcer la protection des données personnelles des citoyens des États membres

Le règlement relatif à la protection des données personnelles a tout d'abord pour ambition de poser des règles plus strictes et précises que ne le faisait la directive de 1995. Ainsi toute entreprise ou organisation collectant des informations personnelles devra-t-elle désormais obtenir le consentement clair et explicite des personnes physiques concernées. C'est le fameux système de l' « opt-in » qui se trouve de la sorte généralisé : chacun devra, par un acte positif tel qu'un « clic » dans une case, consentir à la récolte et à la réutilisation de ses données personnelles. Et, tandis qu'il sera plus aisé de revenir sur son consentement, le règlement consacre le droit pour toute personne d'accéder de façon facilitée aux données la concernant, ainsi qu'aux explications relatives à l'usage fait de ces données. Toutes les informations devront être accessibles de façon simple et claire, tant sur le fond que sur la forme, les députés européens ayant entendu mettre un terme aux politiques de vie privée « en très petits caractères ».

En outre, est consacré un véritable « droit à l'oubli », c'est-à-dire un droit à l'effacement des informations antérieurement diffusées en ligne. Cela permettra, par exemple, à tout individu d'exiger le retrait immédiat de données à caractère personnel divulguées sur un réseau social quelques temps auparavant et dont la publicité est susceptible de lui porter préjudice.

Est également limité le recours au profilage. Celui-ci ne sera possible qu'à condition que la personne en cause y ait consenti, que la loi nationale le permette et qu'il soit nécessaire et proportionné. Cela signifie que chacun pourra refuser qu'un fournisseur de service traite ses données personnelles afin d'établir son profil pour ensuite lui proposer, par exemple, des publicités ciblées. Cette disposition est discutée car elle tend à remettre en cause le modèle économique des sociétés telles que Facebook.

Un autre volet du règlement concerne la protection des mineurs, souvent moins sensibilisés que les majeurs aux risques et conséquences de la diffusion de leurs informations personnelles : dès lors qu'un jeune de moins de 16 ans souhaitera utiliser quelque service du web, celui-ci devra obtenir au préalable l'accord exprès des parents. La limite de 16 ans pourra être abaissée jusqu'à 13 ans par les États afin qu'ils puissent conserver les règles équivalentes déjà souvent en vigueur.

Le nouveau texte consacre encore la règle du « Privacy by design » (respect de la vie privée dès la conception). Cela obligera les entreprises et autres organisations, publiques ou privées, traitant des données personnelles à prendre en compte les exigences relatives à la protection de ces données dès la conception des produits et services, à les intégrer au cœur de tout nouveau projet informatique. Doit également être signalée la norme de la « Security by default » (sécurité par défaut), laquelle imposera à tout organisme de disposer d'un système d'information présentant les fonctionnalités minimales requises en matière de sécurité à toutes les étapes de la gestion de données. Et il faut noter l'obligation mise à la charge des responsables de

traitements de données de respecter des règles de transparence et de traçabilité dites d' « accountability ». Cela implique qu'ils devront mettre en œuvre des mesures appropriées telles que des études d'impact afin d'être en mesure de démontrer que le traitement des données à caractère personnel est effectué dans le respect du règlement.

Enfin, il convient de souligner combien le niveau des sanctions prévues en cas de non-respect de la nouvelle règlementation (jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel total mondial) a vocation à renforcer la portée et l'efficacité de toutes ces dispositions en jouant un véritable rôle dissuasif.

Le deuxième objectif : favoriser le développement du marché numérique unique

Le règlement européen octroie un droit à la « portabilité des données » facilitant le transfert des informations personnelles d'un fournisseur de services à un autre en cas de changement. Grâce à ce nouveau droit, il sera possible, par exemple, de changer de fournisseur de messagerie électronique tout en conservant ses contacts et ses anciens courriels. Pareille disposition a pour but non de protéger les données des utilisateurs mais de stimuler la concurrence sur certains marchés. En effet, un autre objectif porté par le règlement européen est de développer le marché numérique unique, notamment en clarifiant les contraintes juridiques pesant sur les entreprises du secteur, afin de stimuler l'innovation et favoriser la concurrence loyale entre les acteurs.

Le règlement a donc également pour finalité de faciliter les transferts de données au sein du marché intérieur européen, ce qui est en partie contradictoire avec l'objectif par ailleurs affiché de préserver la vie privée des citoyens. L'intention de créer un environnement législatif favorable aux actuels et futurs champions européens du numérique est pour autant pleinement assumée par les instances de l'Union européenne. D'autres dispositifs viennent ainsi la réaliser concrètement, à l'image du nouveau « mécanisme de cohérence ». En prévoyant un ensemble unique de règles valables dans toute l'Union et applicables à toutes les entreprises proposant leurs services au sein de l'Union, le règlement doit prémunir contre les situations de cacophonie juridique entre États qui existaient jusqu'à présent, freinant les échanges transfrontières de données en raison de l'insécurité juridique qu'elles faisaient naître. Et, en soumettant très expressément les entreprises non européennes s'adressant aux consommateurs européens aux mêmes règles que les entreprises européennes, le texte doit permettre une concurrence équitable entre tous ces acteurs.

De plus, tout un pan du nouveau règlement vise à réduire les charges administratives liées au traitement des données personnelles. Notamment, afin de diminuer les coûts et garantir une sécurité juridique renforcée, des décisions uniques devront être prises concernant les affaires transfrontières susceptibles de faire

intervenir plusieurs autorités de contrôle nationales. Ce mécanisme de guichet unique permettra à toute entreprise active au sein de plusieurs États membres de ne traiter qu'avec l'autorité de protection des données de l'État dans lequel elle possède son établissement principal.

Il faut toutefois analyser ces nouveaux avantages en rapport avec les obligations mises à la charge des entreprises afin de renforcer la protection de la vie privée des citoyens européens. Dans l'ensemble, il n'est guère assuré que les acteurs du marché numérique unique seront désormais dans une situation plus simple que celle qu'ils connaissaient sous l'empire de la directive de 1995. Néanmoins, la Commission européenne estime à 2,3 milliards d'euros par an les gains économiques tirés de la nouvelle législation européenne et de la clarification et mise en cohérence du droit en résultant.

Le troisième objectif : établir un cadre juridique européen pour les transferts de données à des fins policières et judiciaires

La directive relative à la protection des données à caractère personnel transmises à des fins de coopération policière et judiciaire, qui constitue le second élément du « paquet législatif », doit remplacer une décision-cadre de 2008 (2008/977/JHA). Son objet est de fixer des normes minimales en matière de protection des individus (victimes, suspects et témoins) dont les données sont traitées à des fins de prévention, de détection et de poursuite d'infractions pénales, cela pour garantir le respect de leurs droits et libertés tout en permettant aux forces de police européennes de coopérer de façon plus efficace qu'auparavant. Jusqu'à présent, les pratiques en matière pénale étaient très différentes d'un État à l'autre, certains donnant la primauté à l'ordre public et à la sécurité contre le droit au respect de la vie privée, d'autres privilégiant ce dernier.

La nouvelle directive intervient dans un contexte difficile en raison des menaces terroristes qui pèsent sur l'Europe. Elle s'efforce néanmoins de rechercher le meilleur équilibre entre des intérêts antagonistes et, surtout, de favoriser la mise en relation des États. En effet, un problème important concernant la lutte contre les attentats terroristes et autres crimes transnationaux est que beaucoup d'États hésitent ou même se refusent à transmettre certaines informations pourtant précieuses. En fixant des normes européennes applicables aux échanges de données personnelles entre autorités répressives, la directive doit renforcer la confiance mutuelle entre les institutions policières et judiciaires des États membres et ainsi favoriser la prévention et la sanction transfrontalière des actes criminels.

Face à la dimension supra-étatique des enjeux impliqués par les nouvelles technologies de l'information et de la communication, l'Europe s'efforce d'être un moteur et de montrer l'exemple, qu'il s'agisse de lutte contre un terrorisme de plus en plus transnational ou de développement de marchés économiques eux-aussi de

plus en plus transnationaux. Le « paquet législatif » relatif à la protection des données personnelles en est une excellente illustration. Et tout aussi importante que la question du contenu de ce « paquet législatif » est celle de son application concrète, tant l'un des problèmes majeurs affectant le droit de l'internet est celui de la faible effectivité des lois qui le constituent. Mais ce ne sera que dans un certain temps qu'il deviendra possible de répondre à cette autre question, un temps qui, d'ailleurs, n'est peut-être pas compatible avec le temps de l'internet.